UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/507,190	09/09/2004	Pim Theo Tuyls	NL 020192	1803

24737 7590 06/22/2009
PHILIPS INTELLECTUAL PROPERTY & STANDARDS
P.O. BOX 3001
BRIARCLIFF MANOR, NY 10510

EXAMINER	
TRAORE, FATOUMATA	
ART UNIT	PAPER NUMBER
2436	
MAIL DATE	DELIVERY MODE
06/22/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/507,190	TUYLS ET AL.	
	Examiner	Art Unit	
	FATOUMATA TRAORE	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 March 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3 and 9-19* is/are rejected.

7)☒ Claim(s) *5-8* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to the amendment filed March 30, 2009. Claims 1-20 have been amended. Claims 1-20 are pending and have been considered below.

Response to Amendment

2. Applicant's arguments, see page 8-9, filed 30, 2009, with respect to the Double patenting rejection have been fully considered and are persuasive. The double patenting rejection has been withdrawn.

3. Applicant's amendments to the claims with respect for the lack of indented elements have been fully considered are entered. The objection to claims 1-20 has been withdrawn.

4. Applicant's amendment, see pages 2-7, filed March 30 2009, with respect to the 35 U.S.C. 101 rejections have been fully considered and did not overcome the rejection because it introduces a new matter as applicant amended the claims using first machine and second machine that do not have support anywhere in the specification. The 35 U.S.C. 101 rejections of the claims 1-20 is maintained.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

6. Claims 1-20 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not

described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. The amendment has introduce a new matter as applicant amended the claims using first machine and second machine that do not have support anywhere in the specification.

Response to Arguments

7. Applicant's arguments filed March 30 2009, respect to the prior art rejection have been fully considered but they are not persuasive. Applicant argues, "*The Office action acknowledges that Herzberg fails to teach a method wherein a first party additionally holds a ..... As is clearly evident, the cited text does not disclose a product of symmetrical polynomials, as specifically claimed in each of the applicants' independent claims. Of particular note, the term 'symmetrical polynomial' does not appear anywhere within Hoffstein . In response the examiner respectfully disagrees and submit that The Office action asserts that Hoffstein discloses "generating a secret key based on the product of two symmetrical polynomials" at column 3, lines 31-46 and FIG. 3. This assertion is incorrect.*"

8. The Examiner respectfully disagrees and submits that Hoffstein was used to show the generation of a secret based on product of two polynomials. However, after further review of the prior arts of record , the examiner submits that Herzberg et al disclose a method of generating a common secret between a first .machine and a second machine, in which wherein the first, machine holds a value Pl and a symmetrical polynomial P(x,y) fixed in the first argument by the value pl, and the first machine performs the steps of: sending the value p1 to the second machine, receiving a value P2 from the second, machine and calculating the common secret S1 by

evaluating the polynomial P(p1, y) in P2, wherein the first, machine additionally holds a value q1 and a symmetrical polynomial Q(x, z) fixed in the first argument by the value q1, and further performs the steps of: sending q1 to the second machine, receiving a value q2 from the second, machine and calculating the secret S1 as Sl=Q(ql, q2).P(Pl, P2)(see column 3, lines 12-50; column 4, line 64 to column 5, line6; column 5, line 50 to column 7, line 27). Therefore, the examiner submits that Herzberg et al teach the limitation of claim 1 as presented and maintains the rejection. The other independent claims 16, 17 and 19 recite similar limitations. Consequently claims 1-4 and 9-20 are still rejected.

9. There is no new ground of rejection when the basic thrust of the rejection remains the same. See In re Kronig, 539 F.2d 1300, 1302-03, 190 USPQ 425,426-27 (CCPA 1976) To the extent that the response to the applicant's arguments may have mentioned new portions of the prior art references, which were not used in the prior office action, this does not constitute new a new ground of rejection. It is clear that the prior art reference is of record and has been considered entirely by applicant. See In re Boyer, 363 F.2d 455,458 n.2,150 USPQ 441,444, n.2 (CCPA 1966) and In re Bush, 296 F.2d 491,496, 131 USPQ 263,267 (CCPA 1961).
The mere fact that additional portions of the same reference may have been mentioned or relied upon does not constitute new ground of rejection. In re Meinhardt, 392, F.2d 273,280, 157 USPQ 270, 275 (CCPA 1968)

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> a. A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person

having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. Claims 1, 9-12,and 16-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Herzberg et al (US 5,202,921) in view of Hoffstein et al (US 6,076,163).

Claims 1, 16, 17 and 19:Herzberg et al discloses a method, a system , a device and a computer program product of generating a common secret between a first party and a second party(abstract; column 2, lines 45-60; column 3 lines 20-40), in which the first party holds a value P1 and a symmetrical polynomial P(x, y) fixed in the first argument by the value p1, and the first party performs the steps of sending the value p1to the second party, receiving a value P2 from the second party and calculating the common secret S1 by evaluating the polynomial P(p1, y) in P2(column 5, line 60 to column7 line26) , characterized in that the first party additionally holds a value q1 and a symmetrical polynomial Q(x, z) fixed in the first argument by the value q1 and further performs the steps of sending q1 to the second party, receiving a value q2 from the second party and calculating the secret S1 as S1=Q(q1, q2).P(P1, P2)(*column 6, Ine 10 to column 7, lines 15*)., but does not explicitly discloses that the secret is generated based on the product of two symmetrical polynomial. However, Hoffstein et al discloses a secure user identification method, system, device and computer program product, which further discloses a step of generating a secret key based on the product of two symmetrical polynomial(column 3, lines 31-46 and Fig. 3). Therefore, it would have been obvious to one having ordinary skills in the art at the time the invention was made to generate a secret based on a product of two polynomial. One would have been motivated

to do so in order to maintain a secure communication by not allowing eavesdroppers to access critical information.

Claim 9: Herzberg et al and Hoffstein et al disclose a method for of generating a private pair of key for enciphering communication between the users as in claim 1 above, and Herzberg et al further discloses that the first party and the second party use a non-linear function on the generated secret S1 and S2, respectively, before using it as a secret key in further communications (column 5, lines 50-60).

Claim 10: Herzberg et al and Hoffstein et al disclose a method for of generating a private pair of key for enciphering communication between the users as in claim 9 above, and Hoffstein et al further discloses that a one-way hash function is applied to the generated secrets S1 and S2(the above described user identification technique can be converted to a digital signature technique by the prover applying a one way hash function to Ag(x) to generate a simulated challenge polynomial) (column 3, lines 30-46). Therefore, it would have been obvious to one having ordinary skills in the art at the time the invention was made to modify the teaching of Herzberg et al such as to use a hash function. One would have been motivated to do so in order to maintain a secure communication by not allowing eavesdroppers to access critical information.

Claim 11: Herzberg et al and Hoffstein et al disclose a method for generating a private pair of key for enciphering communication between the users as in claim 9 above, and Herzberg et al further discloses that the first party and the second party use a non-linear function on the generated secret S1 and S2, respectively, before using it as a secret key in further communications (column 5, lines 60-65).

Claim 12: Herzberg et al and Hoffstein et al disclose a method for generating a private pair of key for enciphering communication between the users as in claim 1 above, and Herzberg et al further discloses that a step of verifying that the second party knows the secret S1 (column 6, lines 20-35).

Claim 18: Herzberg et al and Hoffstein et al disclose a system for of generating a private pair of key for enciphering communication between the users as in claim 17 above, and Herzberg et al further discloses a storage means for storing the polynomial P and the polynomial Q in the form their respective coefficients (column 5, lines 25-40).

12. Claims 2-4 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Herzberg et al (US 5,202,921) in view of Hoffstein et al (US 6,076,163) in further view of Matyas et al (US 5953420).

Claim 2: Herzberg et al and Hoffstein et al disclose a method for generating a private pair of key for enciphering communication between the users as in claim 1 above, while neither of them exclusive discloses a step of generating random numbers. However, Matyas et al discloses a method for establishing an authenticated shared secret value between a pair of users, which further discloses that the first party further performs the steps of obtaining a random number r1 (user A generates a secret value Xla using a pseudorandom number generator) (column 6, lines 15-20), calculating .r1. q1 (generates a public value Y1 from the secret value Xl as Y1 = G^xl mod p) (column 6 lines 20-25), sending r1 .q1 to the second party(each party transmits its own public value Y1 to the other party) (column 6, lines 35-38), receiving r2.q2 from the second party and

calculating the secret S1 as S1=Q(q1, rl.r2.q2).P (pl, p2) (each party generates a value Z2 from the public value Y2 received from the other party and its own secret value X2.as Z2 =Y2^x2 mod p) (column 7, lines 33-45). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of Herzberg et al and Hoffstein et al such as to generate random number in the secret key exchange protocol as taught by Matyas et al. The motivation of doing so would have been against attempts to retrieve the key.

Claim 3: Herzberg et al, Hoffstein et al and Matyas et disclose a method for generating a private pair of key for enciphering communication between the users as in claim 2 above, and Matyas et al further discloses that the first party holds the Value q1 multiplied by an arbitrarily chosen value r (user A generates a secret value Xla using a pseudorandom number generator) (column 6, lines 15- 20), and the product Q (q1, z). P (pl, y) instead of the individual polynomials P (pl, y) and Q (q1, z) (generates a public value Y1 from the secret value Xl as Y1 = G^xl mod p) (column 6 lines 20-25), and the first party performs the steps of calculating r1 .r.q1, sending rl.r.q1 to the second party, receiving r2.r.q2 from the second party and calculating the secret S1 as S1= Q (q1, rl.r2.r.q2). P (pl, p2) (each party generates a value Z2 from the public value Y2 received from the other party and its own secret value X2 as Z2 =Y2^x2 mod p) (column 7, lines 33-45). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of Herzberg et al and Hoffstein et al such as to generate a Secret S1 as taught by Matyas et al. The motivation of doing so would have been against attempts to retrieve the key.

Claims 4, and 20: Herzberg et al and Hoffstein et al disclose a method for generating a private pair of key for enciphering communication between the users as in claims 1 and 16 above, while above, while neither of them exclusive discloses a step of generating the secret key $2. However, Matyas et al discloses a method for establishing an authenticated shared secret value between a pair of users, which further discloses that the second party holds a value P2 and a value q2(Fig. 4, item 400), the symmetrical polynomial P(x, y) fixed in the first argument by the value P2, the symmetrical polynomial Q(x, z) fixed in the first argument by the value q2, and the second party performs the steps of sending q2 to the first party(Fig.7 step 706), receiving ql from the first party (Fig. 7, step 708)and calculating a secret $2 as S2=Q(q2, ql)'P(P2, P1), whereby the common secret has been generated if the secret $2 equals the secret $1 (each party generates a value Z2 from the public value Y2 received from the other party and its own secret value X2 as Z2 =Y2^x2 mod p) (column 7, lines 33-45). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of Herzberg et al and Hoffstein et al such as to generate a secret $1 as taught by Matyas et al. The motivation of doing so would have been against attempts to retrieve the key

13. Claims 13-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Herzberg et al (US 5,202,921) in view of Hoffstein et al (US 6,076,163) in further view of Menezes et al (handbook of applied Cryptography, ISBN 0-8493-8523-7 1997).

Claim 13: Herzberg et al and Hoffstein et al disclose a method for generating a private pair of key for enciphering communication between the users as in claim 12 above, while

neither of them explicitly a step of applying a zero knowledge protocol. However, Menezes et al discloses a similar method, which further discloses that the first party subsequently applies a zero-knowledge protocol to verify that the second party knows the secret S1 (The prover claiming to be A selects a random element from pre-defined set as its secret commitment, and from this computes an associated (public) witness. This provides initial randomness for variation from other protocols runs, and essentially defines a set of questions all of which the prove claims to be able to answer, thereby a priori constraining her forthcoming response. By protocol design, only the legitimate party A, with knowledge of A's secret, is truly capable of answering all the questions, and the answer to any one of these provides no information about A's long-term Secret) (pages 409-410, section (IV)). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of Leighton et al and Hoffstein et al such as to use a zero-knowledge protocol as taught by Menezes et al. The motivation of doing so would have been providing unconditional security.

Claim 14: Herzberg et al and Hoffstein et al disclose a method for generating a private pair of key for enciphering communication between the users as in claim 12 above, while neither of them explicitly a step of applying a commitment- based protocol and Menezes et al discloses a similar method, which further discloses that the first party subsequently applies a commitment-based protocol to verify that the second party knows the secret S1 (*The prover claiming to be A selects a random element from pre-defined set as its secret commitment, and from this computes an associated (public) witness. This provides initial*

randomness for variation from other protocols runs, and essentially defines a set of questions all of which the prove claims to be able to answer, thereby a priori constraining her forthcoming response. By protocol design, only the legitimate party A, with knowledge of A's secret, is truly capable of answering all the questions, and the answer to any one of these provides no information about A's long-term secret) (pages 409-410, section (IV)). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of Herzberg et al and Hoffstein et al such that to use a commitment based protocol as taught by Menezes et al. The motivation of doing so would have been providing unconditional security.

Claim 15: Herzberg et al and Hoffstein et al disclose a method for generating a private pair of key for enciphering communication between the users as in claim 14 above, while neither of them explicitly a step of using a symmetric cipher to encrypt a random challenge. However, Menezes et al disclose a similar method which, further discloses that the second party uses a symmetric cipher to encrypt a random challenge (*b chooses a random r, computes the witness x = h(r) (x demonstrates knowledge of r without disclosing it and computes the challenge e = PA(r, B)) (page 404, section (I))*, and sends the encrypted random challenge to the first party(*B sends the encrypted random challenge to A. A decrypts e to recover r' and B' computes x' = h (r') (page 404, section (I)* and the first party subsequently uses the same symmetric cipher as a commit function to commit himself to a decryption of the encrypted random challenge (*A sends r= r1 to B. B succeeds with unilateral entity authentication of A upon verifying) (page 404, section (I))*. Therefore, it would have been obvious to one of ordinary skill in the art at the time

the invention was made to modify the combined method of Herzberg et al and Hoffstein et al such as to use a symmetric cipher as taught by Menezes et al. The motivation of doing so would have been providing unconditional security.

Allowable Subject Matter

14. Claims 5-8 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fatoumata Traore whose telephone number is (571) 270-1685. The examiner can normally be reached Monday through Thursday from 7:00 a.m. to 4:00 p.m. and every other Friday from 7:30 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nassar G. Moazzami, can be reached on (571) 272 4195. The fax phone number for Formal or Official faxes to Technology Center 2100 is (571) 273-8300. Draft or Informal faxes, which will not be entered in the application, may be submitted directly to the examiner at (571) 270-2685.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group Receptionist whose telephone number is (571) 272-2100.

15. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Friday, June 19, 2009.

/F. T./

Examiner, Art Unit 2436

/David García Cervetti/

Primary Examiner, Art Unit 2436